BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Launching of (electro)mechanical process with user identification from file

Patent number: FR2760874
Publication date: 1998-09-18
Inventor: FRUNEAU PATRICK
Applicant: FDI MATELEC SA (FR)
Classification:
- international: G07C1/00; G07C9/00; E05B49/00
- european: G07C9/00C2B
Application number: FR19970002972 19970311
Priority number(s): FR19970002972 19970311

Abstract of **FR2760874**

The control of authorisation to launch a process is based on electronic keys co-operating with a file of forbidden electronic keys. The electronic key holds all the information necessary for the launching of the process. The ele keys are encoded using a code word linked to a particular process management group. Each key authorisation can decode the key information and determine its originating group. Each key carries a number of passwords to selection of an authorised process. The authorisation centres have a password to permit selection of the electro key and authorise it to launch the process. Forbidden keys are identified from a file.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 760 874**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 02972**

(51) Int Cl[6] : **G 07 C 1/00**, G 07 C 9/00, E 05 B 49/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.03.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.09.98 Bulletin 98/38.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FDI MATELEC SA SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** FRUNEAU PATRICK.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) **NOUCEN.**

(57) Dispositif de lancement de processus dont la vérification de l'identité du demandeur est basée sur la gestion d'un fichier des demandeurs interdits.

L'invention est constituée de clefs électroniques servant à identifier le demandeur de lancement de processus, de lecteurs de clefs électroniques servant à sélectionner le processus à lancer, de centrales d'autorisations servant de centre de décision, et de programmateurs de clefs électroniques servant à exploitation du système par le gestionnaire.

Le dispositif selon l'invention est particulièrement destiné aux systèmes de lancement de processus dont la vérification de l'identité et des niveaux d'autorisations des demandeurs sont nécessaires.

FR 2 760 874 - A1

DESCRIPTION GENERALE

La présente invention concerne un système de lancement de processus dont la vérification de l'identité du demandeur est basée sur la gestion d'un fichier des demandeurs interdits.

L'invention est destinée à toute application de lancement de processus ayant besoin de l'identification du demandeur avant le lancement dudit processus. A titres d'exemples, l'invention s'applique à la commande de processus automatique ou semi-automatique, mécanique ou électromécanique, comme la commande d'un moteur, d'une électrovanne, d'un électro-aimant, d'une serrure ou tout autre système.

Les méthodes mécaniques actuellement utilisées pour le lancement de processus font appel à des clefs mécaniques. Ces clefs, qui par l'intermédiaire d'une serrure, actionnent soit des cames, soit des vannes, soit des interrupteurs électriques ou autres, assurent le lancement du processus.

En cas de perte, ou de vol, la gestion par clefs mécaniques met en oeuvre toute une structure qui va de la personne fautive au serrurier. Dans le cas le plus simple, la personne fautive doit en faire par à son gestionnaire qui doit en faire par au serrurier. Lequel serrurier doit changer toutes les serrures acceptant cette clef perdue ou volée et revoir la hiérarchie des clefs dans le cas où la même clef permet le lancement de plusieurs processus. Une fois cela fait, le gestionnaire doit contacter et changer les clefs de toutes les personnes ayant droit au lancement des mêmes processus que ceux autorisés par la clef perdue ou volée.

De même il existe actuellement des méthodes électroniques utilisées pour le lancement de processus faisant appel à des

clefs électroniques. Ces clefs, qui par l'intermédiaire d'une serrure électronique, actionnent soit des relais, soit des électrovannes, soit des transistors ou autres, assurent le lancement du processus.

Comme pour les clefs mécaniques, en cas de perte ou de vol, il faut que la personne fautive avertisse son gestionnaire. Cette personne gérant le système doit passer sur chacune des serrures électroniques pour invalider la clef électronique perdue ou volée, puis programmer une nouvelle clef électronique et la valider sur chacune des serrures électroniques. En cas de perte ou de vol du programmateur de clefs électroniques, le système n'est plus sécurisé car la duplication et la création de clef électronique sont aisément possible.

Il faut noter que la duplication de clef électronique demande une mise en oeuvre plus complexe que son homologue mécanique mais est possible. Pour éviter au gestionnaire le déplacement sur toutes les serrures électroniques, celles-ci sont reliées par un réseau local dédié ce qui permet une gestion centralisée.

Que les systèmes soient mécaniques ou électroniques, en cas de malveillance ou de vandalisme, on peut lancer le processus de façon relativement aisé. En démontant ou cassant le carter de la serrure mécanique ou électronique on a accès aux éléments mécaniques ou électromécaniques qui lancent le processus.

Un autre problème sur les systèmes mécaniques ou électroniques est que les fabriquants et les installateurs du matériel qui, pour leurs tests possèdent des clefs donnant accès au lancement de processus.

Sur les systèmes électroniques, la programmation des clefs électroniques se fait par un programmateur qui demande l'intermédiaire d'un ordinateur ou d'un terminal pour pouvoir être opérationnel. De même des serrures électroniques demandent

l'intermédiaire d'un ordinateur ou d'un terminal pour leur utilisation et programmation. Ce matériel nécessaire à l'exploitation du système est lourd, coûteux et d'une utilisation complexe.

On voit que ces systèmes, mécaniques ou électroniques demandent une installation, une gestion et une maintenance contraignante.

L'invention qui résout les contraintes et les inconvénients de ces systèmes a une architecture basée sur les éléments suivants: les clefs électroniques, les lecteurs de clefs électroniques, les centrales d'autorisations et les programmateurs de clefs électroniques.

Selon l'invention basée sur l'organisation de la gestion d'un fichier des interdits il n'est pas nécessaire de programmer et de maintenir à jour un fichier des clefs électroniques autorisées à lancer les processus.

Pour éviter d'avoir accès au lancement du processus en cas de démontage ou de vandalisme sur les lecteurs de clefs électroniques, ceux-ci ne possèdent pas d'éléments permettant le lancement direct du processus. Seules les centrales d'autorisations possèdent le moyen de lancer des processus. Les lecteurs de clefs électroniques ont uniquement pour fonction la vérification de la cohérence du contenu des clefs électroniques et la liaison avec les centrales d'autorisations. La liaison entre la serrure électronique et la centrale d'autorisation se fait de façon encodée pour éviter le piratage de la ligne. La liaison avec les centrales d'autorisations se fait sur 2 fils servant à la fois de ligne d'alimentation des lecteurs de clef électronique et de ligne de communication avec les centrales d'autorisations.

Dans le cas de clef électronique à contacts, le lecteur de clef électronique est remplacé par un système de contact uniquement mécanique. Cela accroît la sécurité du système car le démontage du lecteur de clef électronique ne donne pas d'accès à

l'électronique du système. Avec ce lecteur de clefs électroniques uniquement mécanique, la centrale d'autorisation se substitue au lecteur de clef électronique et effectue elle-même la vérification de la cohérence du contenu des clefs électroniques.

Pour éviter une installation demandant la réalisation d'un réseau local, les clefs électroniques permettent le stockage de toutes les informations relatives à leurs autorisations de lancement de processus. Grâce aux informations contenues dans les clefs électroniques, les centrales d'autorisations peuvent interdire ou autoriser le lancement de processus sans avoir besoin d'un fichier des clefs électroniques en service. Ces informations seront désignées par le vocabulaire, passe, autorisation d'accès, identification, exemplaire, groupe horaire, début de validité, fin de validité et caractères de contrôles. L'explication de ce vocabulaire se fera au fur et à mesure de la description du système. Ces informations de gestion sont enregistrées dans les clefs électroniques par le gestionnaire au moment de leur programmation ce qui permet une gestion centralisée. Les centrales d'autorisation n'ayant pas de fichier à programmer, cela évite l'installation d'un réseau pour avoir une gestion centralisée et garder leurs fichiers à jour.

Pour éviter qu'un gestionnaire puisse avoir accès à d'autres processus que ceux placés sous sa gestion, le système fait appel à des mots d'encodages déterminés par le gestionnaire. Les clefs électroniques seront encodées à l'aide de ce mot d'encodage déterminé par le gestionnaire. Seules les centrales d'autorisations programmées pour reconnaître ce mot d'encodage pourront accepter les clefs électroniques ayant été encodées par ce même mot d'encodage et autoriser le lancement du processus demandé. Ce mot d'encodage propre au gestionnaire interdit les clefs électroniques créées par le fabriquant ou l'installateur au moment des tests. De même les clefs électroniques créées par un autre gestionnaire seront interdites.

Pour éviter qu'un cas de perte ou de vol du programmateur de clef il soit possible de créer des clefs électroniques, celui-ci ne possède ni ne mémorise le mot d'encodage. Le mot d'encodage devra être saisi sur le programmateur par le gestionnaire avant la programmation des clefs électroniques.

Pour éviter d'avoir à demander l'intermédiaire d'un ordinateur ou d'un terminal pour programmer les clefs électroniques et programmer les centrales d'autorisations, on utilise un petit terminal portable alimenté par batterie. Ce terminal portable possède, un clavier alphanumérique, un écran, un lecteur/programmateur de clefs électronique et une liaison sans fil (infrarouge ou radiofréquence). En mode autonome, le terminal portable permet la programmation des clefs électroniques. Par contre pour programmer les centrales d'autorisations, les écrans et les informations de gestions sont transmis par les centrales d'autorisations à travers la liaison sans fil. Le fait que le terminal portable ne possède pas les écrans et les informations de gestions des centrales d'autorisations permet de limiter la taille, l'encombrement et augmenter le temps d'autonomie du terminal portable.

Pour sélectionner les processus pouvant être lancés par les clefs électroniques avec des centrales d'autorisations n'ayant pas de fichier, on utilise les notions de passe et d'autorisation d'accès. La notion de passe permet une sélection au niveau des centrales d'autorisations. La notion d'autorisation d'accès permet une sélection au niveau des processus car les centrales d'autorisations peuvent gérer plusieurs processus. A chaque processus contrôlé par une centrale d'autorisation, correspond un lecteur de clefs électroniques et un numéro d'autorisation d'accès. Les clefs électroniques possèdent une zone de données réservée à un numéro de passe et une zone de données réservée aux numéros d'autorisations d'accès. Les centrales d'autorisations possèdent une zone de données réservée aux numéros de passe et une zone de données réservée aux numéros d'autorisations d'accès. Les

centrales d'autorisations qui mémorisent plusieurs numéros de passes permettent à une clef électronique de pouvoir lancer des processus distribués sur plusieurs centrales d'autorisations. Les clefs électroniques mémorisent plusieurs numéros d'autorisation d'accès pour pouvoir lancer plusieurs processus. Pour qu'un processus soit lancé il faut que le numéro d'autorisation d'accès du processus corresponde à un des numéros d'autorisations d'accès de la clef électronique.

Pour éviter d'avoir à programmer toutes les clefs électroniques autorisées dans toutes les centrales d'autorisations, celles-ci font uniquement une gestion des clefs électroniques interdites avec la notion d'identification et d'exemplaire. Les clefs électroniques possèdent une zone de données réservée à un numéro d'identification et à un numéro d'exemplaire. Pour toutes les clefs électroniques qui effectuent une demande de lancement de processus, la centrale d'autorisation vérifie que le numéro d'identification et le numéro d'exemplaire de la clef électronique n'est pas présent dans son fichier des clefs électroniques interdites. Si le numéro d'identification et le numéro d'exemplaire de la clef électronique sont présents dans le fichier des clefs électroniques interdites, la demande de lancement de processus sera refusée.

Pour éviter au gestionnaire un déplacement sur les sites, dans le cas de perte ou de vol des clefs électroniques, la centrale d'autorisation effectue une mise à jour automatique de son fichier des clefs électroniques interdites. Pour effectuer cette mise à jour, les centrales d'autorisation utilisent le numéro d'identification et le numéro d'exemplaire. Lorsqu'une demande de lancement de processus est effectuée avec une clef électronique ayant le numéro d'identification i et le numéro d'exemplaire e supérieur à 1, le numéro d'identification i et le numéro d'exemplaire e-1 sont enregistrés dans le fichier des clefs électroniques interdites. La centrale d'autorisation interdit alors le lancement de processus par toutes les clefs

électroniques ayant le même numéro d'identification et ayant un numéro d'exemplaire inférieur ou égal à ceux présent dans son fichier de clefs électroniques interdites. Lors de leurs première mise en service, les clefs électroniques sont programmées avec le numéro d'exemplaire e = 1. Pour toutes demandes de lancement de processus effectuées avec une clef électronique ayant le numéro d'exemplaire e = 1, la centrale d'autorisation ne modifie pas son fichier des clefs électroniques interdites.

Pour limiter dans le temps l'autorisation de lancement de processus, on utilise la notion de début et de fin de validité. Les clefs électroniques possèdent une zone de données réservée pour les dates de début et de fin de validité. Les centrales d'autorisations utilisent ces dates de début et de fin de validité par comparaison avec la date (dans tout le texte on entend par date les jours du mois, les mois et les années) de son horloge interne pour autoriser ou interdire le lancement un processus. La date de début de validité permet de créer et de distribuer les clefs électroniques aux utilisateurs avant la date donnant droit au lancement de processus. La date de fin de validité permet d'interdire les clefs électroniques dans le cas où les utilisateurs ne rendent pas les clefs électroniques au gestionnaire.

Pour limiter les horaires d'autorisation de lancement de processus jour par jour, on utilise la notion de groupe horaire. Les clefs électroniques possèdent une zone de données réservée à un numéro de groupe horaire. Les centrales d'autorisation possèdent une zone de données réservée pour des tables d'horaires. Chaque table d'horaire est associée à un numéro de groupe horaire. Le numéro de groupe horaire est utilisé par les centrales d'autorisations pour sélectionner une des tables donnant les horaires pendant lesquelles une clef électronique a le droit de lancer un processus. Ces tables d'horaires définissent les horaires d'autorisation de lancement des processus sur une semaine. Les jours de cette semaine sont

découpés en tranches donnant les heures et minutes de début et de fin d'autorisation de lancement des processus. Dans le cas de clef électronique disposant de suffisamment de mémoire, la table d'horaire est enregistrée par la clef électronique.

Les centrales d'autorisations utilisent cette table d'horaire par comparaison avec l'heure (dans tout le texte on entend par l'heure les heures et les minutes) de son horloge interne pour autoriser ou interdire le lancement un processus.

La notion de caractères de contrôle est utilisée pour vérifier la validité et de cohérence des informations de la clef électronique. Cela peut aller du simple LRC à une signature informatique.

Certains processus doivent pouvoir être lancés à distance en utilisant des technologies infrarouges ou radiofréquences et d'autre pouvoir être lancés à proximité en utilisant des technologies de proximités ou de contacts. Cette demande est aussi faite pour la rénovation de site où l'on ne peut pas changer les lecteurs de clefs électroniques qui utilisent des moyens différents pour la communication avec les clefs électroniques. Les clefs électroniques peuvent pouvoir regrouper plusieurs technologies différentes pour la communication avec les lecteurs, cela leur permet d'accéder à des processus distants ou proches suivant les cas.

DESCRIPTION DES FIGURES

Les éléments selon l'invention des figures 1 et 2 donnent une présentation générale de la structure du système avec les clefs électroniques « CLEL » possédant un numéro de groupe horaire « GRHO » et des centrales d'autorisation possédant des tables d'horaires « TAHO ».

Les éléments selon l'invention des figures 3 et 4 donnent une présentation générale de la structure du système avec les clefs électroniques « CLEL » possédant une table horaire « TAHO » et des centrales d'autorisation sans tables d'horaires.

Les éléments selon l'invention des figures 5 et 6 donnent un exemple d'application particulière de l'invention.

Sur la figure 1 on retrouve la clef électronique « CLEL » encodée par le mot d'encodage « MOEN » et possédant les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

Sur la figure 2 on retrouve la centrale d'autorisation « CEAU» qui possède les informations suivantes.

- sa liste de n numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN ».
- son horloge « HORL ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- sa liste de n tables d'horaires « TAHO ».

Avec les éléments selon l'invention des figures 1 et 2, pour qu'un processus puisse être lancé, il faut que les conditions suivantes soient remplies.

1°) Le caractère de contrôle « CACO » de la clef électronique « CLEL » de la figure 1 doit être valide pour que les lecteurs de clefs électroniques « LE-x » de la figure 2 transmettent le contenu des clefs électroniques « CLEL » de la figure 1 aux centrales d'autorisations « CEAU » de la figure 2.

2°) La centrale d'autorisation « CEAU » de la figure 2, après réception du contenu de la clef électronique « CLEL » de la figure 1, vérifie de nouveau le caractère de contrôle « CACO » de la clef électronique « CLEL » de la figure 1 qui doit être valide.

3°) Le mot d'encodage « MOEN » de la centrale d'autorisation « CEAU » de la figure 2 doit lui permettre de décoder les données de la clef électronique « CLEL » de la figure 1. Pour cela il faut que le mot d'encodage « MOEN » de la clef électronique « CLEL » de la figure 1 soit le même que celui de la centrale d'autorisation « CEAU » de la figure 2.

4°) Le numéro de passe « PASS » de la clef électronique « CLEL » de la figure 1 doit correspondre à l'un des n numéros de passe « PASS » de la centrale d'autorisation « CEAU » de la figure 2.

5°) Le numéro d'identification « IDEN » de la clef électronique « CLEL » de la figure 1 ne doit pas être présent dans la zone d'identification « IDEN » du fichier des interdits « FIIN » de la centrale d'autorisation « CEAU » de la figure 2. Si le numéro d'identification « IDEN » de la clef électronique « CLEL » de la figure 1 est présent dans la zone d'identification « IDEN » du fichier des interdits « FIIN » de la centrale d'autorisation « CEAU » de la figure 2, le numéro d'exemplaire « EXAM » de la clef électronique « CLEL » de la figure 1 doit être supérieur au numéro d'exemplaire « EXAM » du fichier des interdits « FIIN » de la centrale d'autorisation « CEAU » de la figure 2.

6°) La date de début de validité « DEVA » de la clef électronique « CLEL » de la figure 1 doit être supérieure ou égale à la date de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 2 et la date de fin de validité « FIVA » de la clef électronique « CLEL » de la figure 1 doit être inférieure ou égale à la date de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 2.

7°) Le numéro du groupe horaire « GRHO » de la clef électronique « CLEL » de la figure 1 doit faire référence à un des numéros des tables d'horaires « TAHO » de la centrale d'autorisation « CEAU » de la figure 2. Dans cette table d'autorisation « TAHO » de la centrale d'autorisation « CEAU » de la figure 2, il doit y avoir, pour le jour de la semaine correspondant à celui de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 2 une des n tranches de ce jour donnant des heures valides. Pour être valide on doit avoir l'heure de début de validité de la tranche supérieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 2 et l'heure de fin de validité inférieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 2.

8°) Le lecteur de clefs électroniques « LE-x » (1 <= x =< n) de la figure 2, par lequel la demande de lancement de processus a été effectuée, est lié au niveau de la centrale d'autorisation « CEAU » de la figure 2 au processus « PR-x » (1 <= x =< n) de la figure 2 par un numéro d'autorisation d'accès 1 <= x =< n. Ce numéro doit correspondre à l'un des n numéros d'autorisations d'accès « AUAC » de la clef électronique « CLEL » de la figure 1.

Dans la figure 3, la clef électronique « CLEL » ne possède pas de numéro de groupe horaire « GRHO » comme c'est le cas dans la clef électronique « CLEL » de la figure 1 mais une table d'horaire « TAHO ». Sur la figure 3, la clef électronique « CLEL » encodée par le mot d'encodage « MOEN » possède donc les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- sa table d'horaire « TAHO ».
- sa liste de n numéro autorisations d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

Dans la figure 4, la centrale d'autorisation « CEAU » ne possède pas de tables d'horaires « TAHO » comme c'est le cas dans la centrale d'autorisation « CEAU » de la figure 2. Sur la figure 4 la centrale d'autorisation « CEAU» possède donc les informations suivantes.

- sa liste de n numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN ».
- son horloge « HORL ».
- sa liste de n numéro autorisations d'accès « AUAC ».

Avec les éléments selon l'invention des figures 3 et 4, pour qu'un processus puisse être lancé, on retrouve les mêmes conditions que les éléments selon l'invention des figures 1 et 2 avec une différence sur la condition 7°) qui devient la condition suivante.

7°) Dans la table d'autorisation « TAHO » de la clef électronique « CLEL» de la figure 3, il doit y avoir, pour le jour de la semaine correspondant à celui de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 4, une des n tranches de ce jour donnant des heures valides. Pour être valide on doit avoir l'heure de début de validité de la tranche supérieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 3 et l'heure de fin de validité inférieure ou égale à l'heure de l'horloge « HORL » de la centrale d'autorisation « CEAU » de la figure 3.

Les éléments selon l'invention, avec la structure des figures 1 et 2, des figures 5 et 6 donnent un exemple d'application particulière de l'invention.

La figure 5 représente un site sous la responsabilité d'un gestionnaire « G-1 ».

La centrale d'autorisation « CEAU-1 » de la figure 5 possède les informations suivantes.

- sa liste de 2 numéros de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN-1 ».
- son horloge « HORL ».
- sa liste de 2 numéros autorisations d'accès « AUAC ».
- sa liste de 2 tables d'horaires « TAHO ».

La centrale d'autorisation « CEAU-2 » de la figure 5 possède les informations suivantes.

- sa liste de 1 numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN-1 ».
- son horloge « HORL ».
- sa liste de 1 numéro autorisations d'accès « AUAC ».
- sa liste de 1 table d'horaires « TAHO ».

La clef électronique « CLEL-1 » de la figure 5 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».

- sa liste de 1 numéro autorisation d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

La clef électronique « CLEL-2 » de la figure 5 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».
- sa liste de 2 numéros autorisations d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

La figure 6 représente un site sous la responsabilité d'un gestionnaire « G-2 ».

La centrale d'autorisation « CEAU-1 » de la figure 6 possède les informations suivantes.

- sa liste de 1 numéro de passe « PASS ».
- son fichier d'interdit « FIIN ».
- son mot d'encodage « MOEN-2 ».
- son horloge « HORL ».
- sa liste de 3 numéros autorisations d'accès « AUAC ».
- sa liste de 1 table d'horaires « TAHO ».

La clef électronique « CLEL-1 » de la figure 6 encodée par le mot d'encodage « MOEN-1 » possède les informations suivantes.

- son numéro de passe « PASS ».
- son numéro d'identification « IDEN ».
- son numéro d'exemplaire « EXAM ».
- sa date de début de validité « DEVA ».
- sa date de fin de validité « FIVA ».
- son numéro de groupe horaire « GRHO ».

- sa liste de 3 numéros autorisations d'accès « AUAC ».
- ses caractères de contrôle « CACO ».

Les lecteurs électroniques « LE-x » des figures 5 et 6 sont capables de vérifier les caractères de contrôle « CACO » des clefs électroniques « CLEL-x » des figures 5 et 6. Les caractères de contrôle étant vérifiés, le contenu des clefs électroniques est envoyé aux centrales d'autorisations. A ce niveau, les lecteurs électroniques « LE-x » des figures 5 et 6 ne font pas de différences entre le gestionnaire « G-1 » de la figure 5 et le gestionnaire « G-2 » de la figure 6.

Les centrales d'autorisations « CEAU-x » des figures 5 et 6, après réception du contenu des clefs électroniques « CLEL-x » de la figure 5 et 6, vérifient de nouveau le caractère de contrôle « CACO » des clefs électroniques « CLEL-x » de la figure 5 et 6, qui doit être valide. A ce niveau, les centrales d'autorisations « CEAU-x » des figures 5 et 6 ne font pas de différence entre le gestionnaire « G-1 » de la figure 5 et le gestionnaire « G-2 » de la figure 6.

Les centrales d'autorisations « CEAU-x » de la figure 5 qui possèdent le mot d'encodage « MOEN-1 » ne savent décoder que les clefs électroniques « CLEL-x » de la figure 5 qui sont encodées avec le même mot d'encodage « MOEN-1 ». De même les centrales d'autorisations « CEAU-x » de la figure 6 qui possèdent le mot d'encodage « MOEN-2 » ne savent décoder que les clefs électroniques « CLEL-x » de la figure 5 qui sont encodées avec le même mot d'encodage « MOEN-2 ». L'utilisation du mot d'encodage dans le système permet aux centrales d'autorisations « CEAU-x » des figures 5 et 6 de faire la différence entre le gestionnaire « G-1 » de la figure 5 qui utilise le mot d'encodage « MOEN-1 » et le gestionnaire « G-2 » de la figure 6 qui utilise le mot d'encodage « MOEN-2 ».

La clef électronique « CLEL-1 » de la figure 5 qui possède le numéro de passe « PASS 225 » est reconnue par la centrale d'autorisation « CEAU-1 » de la figure 5 qui possède le même numéro de passe « PASS 225 » mais pas par la centrale d'autorisation « CEAU-2 » de la figure 5 qui ne possède pas le

numéro de passe « PASS 225 ». La clef électronique « CLEL-2 » de la figure 5 qui possède le numéro de passe « PASS 245 » est reconnue par la centrale d'autorisation « CEAU-1 » et par la centrale d'autorisation « CEAU-2 » de la figure 5 qui possèdent le numéro de passe « PASS 245 ». La clef électronique « CLEL-1 » de la figure 6 qui possède le numéro de passe « PASS 842 » est reconnue par la centrale d'autorisation « CEAU-1 » de la figure 6 qui possède le même numéro de passe « PASS 842 ». L'utilisation du numéro de passe dans le système permet de limiter certaines clefs électroniques à certaines centrales d'autorisations.

Le numéro d'identification « IDEN 185 » et d'exemplaire « EXAM 4 » présent dans le fichier des interdits « FIIN » des centrales d'autorisations « CEAU-1 et CEAU-2 » de la figure 5 interdit le lancement de processus par toutes les clefs électroniques perdues ou volées ayant le numéro d'identification « IDEN 185 » et un numéro d'exemplaire « EXAM compris de 1 à 4 ». De même le numéro d'identification « IDEN 120 » et d'exemplaire « EXAM 1 » présent dans le fichier des interdits « FIIN » des centrales d'autorisations « CEAU-1 » de la figure 6 interdit le lancement de processus par la clef électronique perdue ou volée ayant le numéro d'identification « IDEN 120 » et le numéro d'exemplaire « EXAM 1 ». L'utilisation du numéro d'identification et du numéro d'exemplaire permet d'avoir un fichier d'interdit mis à jour automatiquement par les centrales d'autorisations selon la méthode expliquée dans la description générale de l'invention.

Les dates de début et de fin de validité « DEVA » et « FIVA » des clefs électroniques « CLEL-x » des figures 5 et 6 définissent la période pendant laquelle ces clefs électroniques ont droit au lancement de processus. L'utilisation des dates de validité permet de limiter au niveau mensuel et annuel les clefs électroniques.

Les horaires qui définissent sur une semaine le droit au lancement de processus de la clef électronique « CLEL-1 » de la figure 5 ayant le groupe horaire « GRHO 2 » sont donnés par la table d'horaires « TAHO 2 » de la centrale d'autorisation

« CEAU-1 » de la figure 5. Les horaires qui définissent sur une semaine le droit au lancement de processus de la clef électronique « CLEL-2 » de la figure 5 ayant le groupe horaire « GRHO 1 » sont donnés par la table d'horaires « TAHO 1 » des centrales d'autorisations « CEAU-1 et CEAU-2» de la figure 5. Les horaires qui définissent sur une semaine le droit au lancement de processus de la clef électronique « CLEL-1 » de la figure 6 ayant le groupe horaire « GRHO 1 » sont donnés par la table d'horaires « TAHO 1 » de la centrale d'autorisation « CEAU-1 » de la figure 6. L'utilisation des tables d'horaires permet de limiter au niveau horaire et hebdomadaire les clefs électroniques.

La clef électronique « CLEL-1 » de la figure 5 dont les autorisations d'accès sont « AUAC 2 », peut lancer le processus « PR-2 » de la centrale d'autorisation « CEAU-1 » de la figure 5. La clef électronique « CLEL-2 » de la figure 5 dont les autorisations d'accès sont « AUAC 1 et 3 », peut lancer le processus « PR-1 » de la centrale d'autorisation « CEAU-1 » de la figure 5 et le processus « PR-3 » de la centrale d'autorisation « CEAU-2 » de la figure 5. La clef électronique « CLEL-1 » de la figure 6 dont les autorisations d'accès sont « AUAC 1, 2 et 3 », peut lancer les processus « PR-1, PR-2 et PR-3 » de la centrale d'autorisation « CEAU-1 » de la figure 6. L'utilisation d'autorisation permet de limiter les processus pouvant être lancé par une clef électronique.

REVENDICATIONS

1. Système de contrôle de lancement de processus caractérisé en ce qu'il comporte une gestion des clefs électroniques basée sur la gestion d'un fichier des clefs électroniques interdites.

2. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les clefs électroniques, pour permettre une gestion basée sur un fichier des interdits, comportent toutes les informations nécessaires à l'autorisation du lancement du processus.

3. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques sont encodées à l'aide d'un mot d'encodage « MOEN » pour permettre une différenciation du patrimoine des gestionnaires.

4. Système de contrôle de lancement de processus selon les revendications 1 à 3 caractérisé en ce que les centrales d'autorisations possèdent un moyen de décodage « MOEN » pour permettre le décodage des clefs électroniques encodées et la différenciation du patrimoine des gestionnaires.

5. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques possèdent un moyen « PASS » pour permettre une sélection des processus autorisés au niveau des centrales d'autorisations.

6. Système de contrôle de lancement de processus selon les revendications 1, 2 et 5 caractérisé en ce que les centrales d'autorisations possèdent des moyens « PASS » pour permettre une sélection des clefs électroniques et autoriser la clef électronique à lancer des processus au niveau des centrales d'autorisations.

7. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent un moyen « IDEN » permettant d'identifier les clefs électroniques interdites.

8. Système de contrôle de lancement de processus selon les revendications 1, 2 et 7 caractérisé en ce que les clefs électroniques comportent un moyen « EXAM » permettant de déterminer l'exemplaire de la clef électronique.

9. Système de contrôle de lancement de processus selon les revendications 1, 2, 7 et 8 caractérisé en ce que les centrales d'autorisations comportent dans le fichier des interdits « FIIN » d'un moyen « IDEN » permettant d'identifier les clefs électroniques interdites.

10. Système de contrôle de lancement de processus selon les revendications 1, 2, 7, 8 et 9 caractérisé en ce que les centrales d'autorisations comportent dans le fichier des interdits « FIIN » d'un moyen « EXAM » permettant de déterminer l'exemplaire de la clef électronique.

11. Système de contrôle de lancement de processus selon les revendications 1, 2, 7, 8, 9 et 10 caractérisé en ce que les centrales d'autorisations utilisent les informations d'identification « IDEN » et d'exemplaire « EXAM » des clefs électroniques pour effectuer une mise à jour automatique du fichier des clefs électroniques interdites.

12. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une date de début de validité « DEVA » et une date de fin de validité « FIVA » permettant de limiter dans le temps les droits, des clefs électroniques, au lancement des processus.

13. Système de contrôle de lancement de processus selon les revendications 1, 2 et 12 caractérisé en ce que les centrales d'autorisation comportent une horloge « HORL » donnant la date courante pour limiter dans le temps les droits, des clefs électroniques, au lancement des processus.

14. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une table d'horaires « TAHO » permettant de limiter de façon hebdomadaire et à la minutes près les droits, des clefs électroniques, au lancement des processus.

15. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent un numéro de groupe horaire « GRHO » permettant de limiter de façon hebdomadaire et à la minutes près les droits, des clefs électroniques, au lancement des processus.

16. Système de contrôle de lancement de processus selon les revendications 1, 2 et 15 caractérisé en ce que les centrales d'autorisation utilisent l'information de groupe horaire « GRHO » des clefs électroniques pour sélectionner une des tables d'horaires « TAHO ».

17. Système de contrôle de lancement de processus selon les revendications 1, 2, 15 et 16 caractérisé en ce que les centrales d'autorisation comportent des tables d'horaires « TAHO » permettant de limiter de façon hebdomadaire et à la minutes près les droits, des clefs électroniques, au lancement des processus.

18. Système de contrôle de lancement de processus selon les revendications 1, 2, 14, 15, 16, et 17 caractérisé en ce que les centrales d'autorisation comportent une horloge « HORL » donnant l'heure courante pour limiter de façon hebdomadaire et à la minute près les droits, des clefs électroniques, au lancement des processus.

19. Système de contrôle de lancement de processus selon les revendications 1 et 2 caractérisé en ce que les clefs électroniques comportent une liste de numéros des autorisations d'accès « AUAC » pour sélectionner les processus auxquels ont droit les clefs électroniques.

20. Système de contrôle de lancement de processus selon les revendications 1, 2 et 19 caractérisé en ce que les centrales d'autorisations comportent une liste des numéros des autorisations d'accès « AUAC » pour associer les lecteurs de clef électroniques aux processus et sélectionner les processus auxquels ont droit les clefs électroniques.

21. Système de contrôle de lancement de processus caractérisé en ce que les clefs électroniques ayant accès à des lecteurs de technologies « proches » (contacts, proximité, magnétique) et à des lecteurs de technologies « distante » (infrarouge, radiofréquence) comportent un moyen technique « proche » et un moyen technique « distant » pour transmettre leur identification et les données qu'elles contiennent.

22. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les lecteurs de clefs électroniques ayant une technologie « proche » de contacts, sont réalisés par des moyens uniquement mécaniques.

23. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les lecteurs de clefs électroniques, interface utilisateurs et les centrales d'autorisations, centre de décision, sont des fonctions séparées.

24. Système de contrôle de lancement de processus selon la revendication 1 caractérisé en ce que les terminaux portables possèdent un lecteur/programmateur de clefs électroniques.

25. Système de contrôle de lancement de processus selon les revendications 1 et 24 caractérisé en ce que les terminaux portables possèdent une liaison sans fil pour la communication avec les centrales d'autorisations.

26. Système de contrôle de lancement de processus selon les revendications 1, 24 et 25 caractérisé en ce que les terminaux portables ne possèdent pas les écrans et les informations de gestions des centrales d'autorisations.

27. Système de contrôle de lancement de processus selon les revendications 1, 24, 25 et 26 caractérisé en ce que les terminaux portables ne mémorisent pas le mot d'encodage des clefs électroniques.

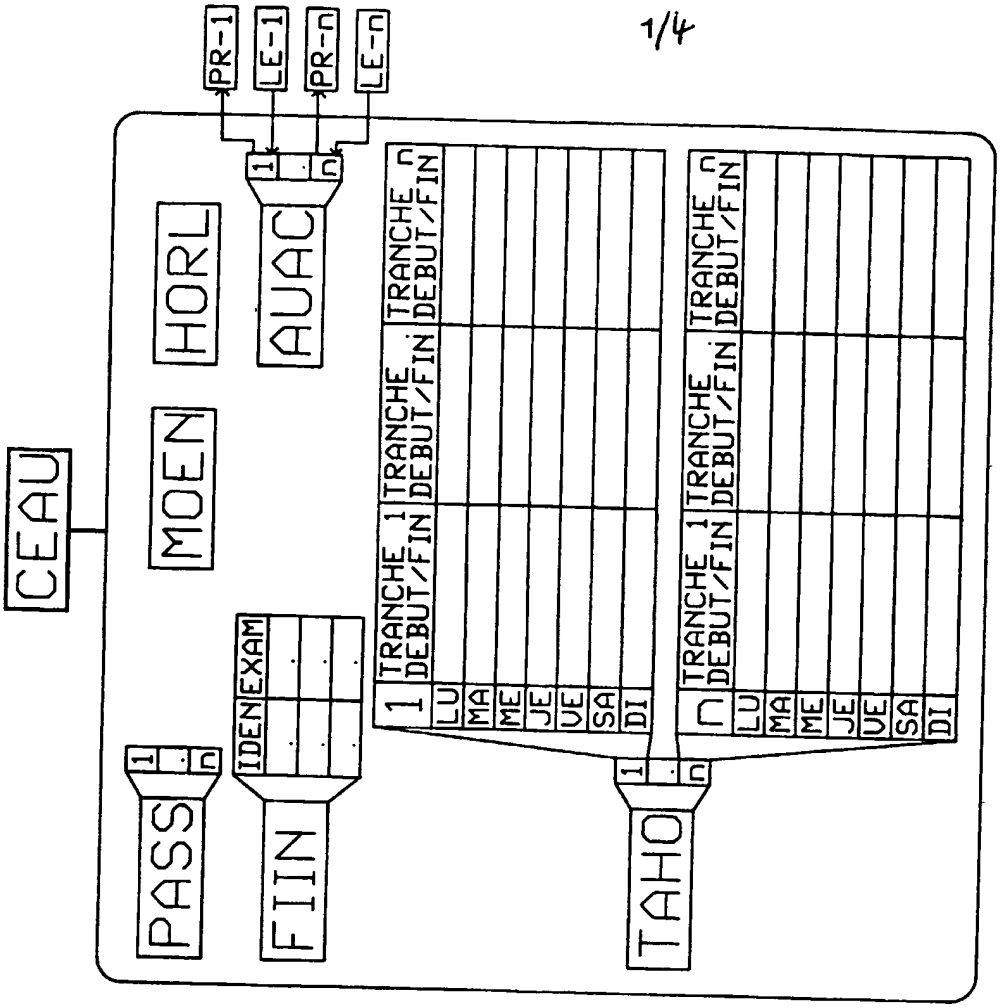
PR-1
LE-1
PR-n
LE-n
CEAU
MOEN
HORL
AUAC
1
n
TRANCHE 1 DEBUT/FIN
TRANCHE DEBUT/FIN
TRANCHE n DEBUT/FIN
LU
MA
ME
JE
VE
SA
DI
IDEN
EXAM
PASS
FIIN
TAHO

FIG 2

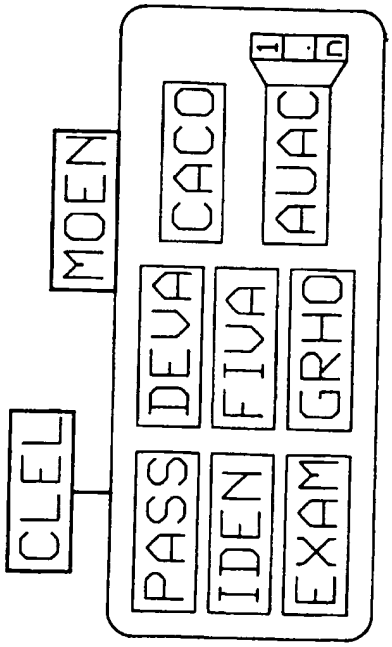
CLEL
MOEN
PASS
IDEN
EXAM
DEVA
FIVA
GRHO
CACO
AUAC
1
n

FIG 1

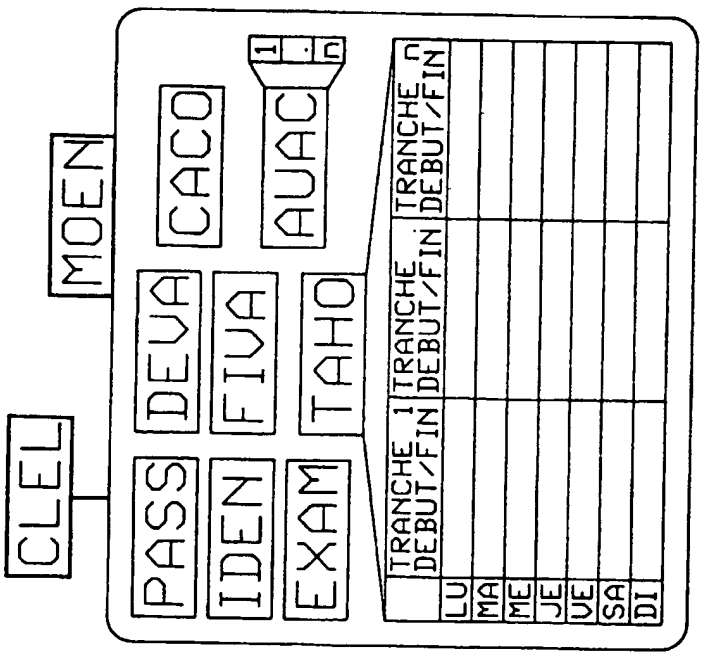
CLEL
MOEN
PASS
IDEN
EXAM
DEVA
FIVA
TAHO
CACO
AUAC
1
n
TRANCHE 1 DEBUT/FIN
TRANCHE DEBUT/FIN
TRANCHE n DEBUT/FIN
LU
MA
ME
JE
VE
SA
DI

FIG 3

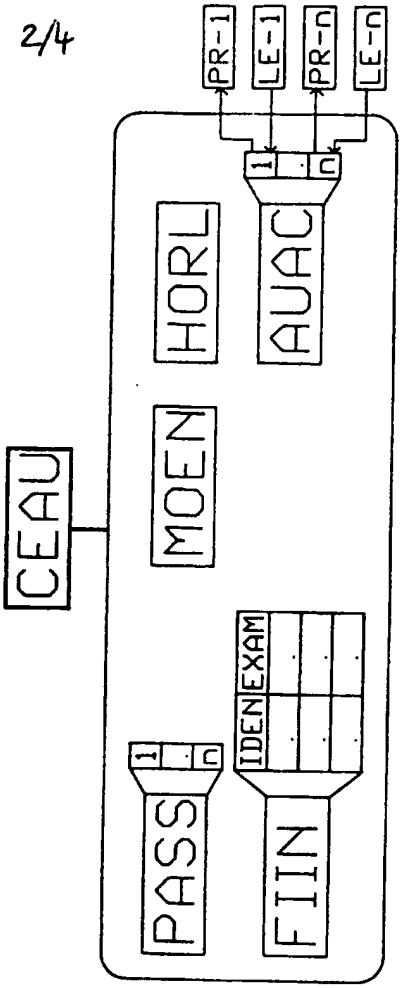
CEAU
MOEN
HORL
AUAC
PASS
FIIN
IDEN
EXAM
1
n
PR-1
LE-1
PR-n
LE-n

FIG 4

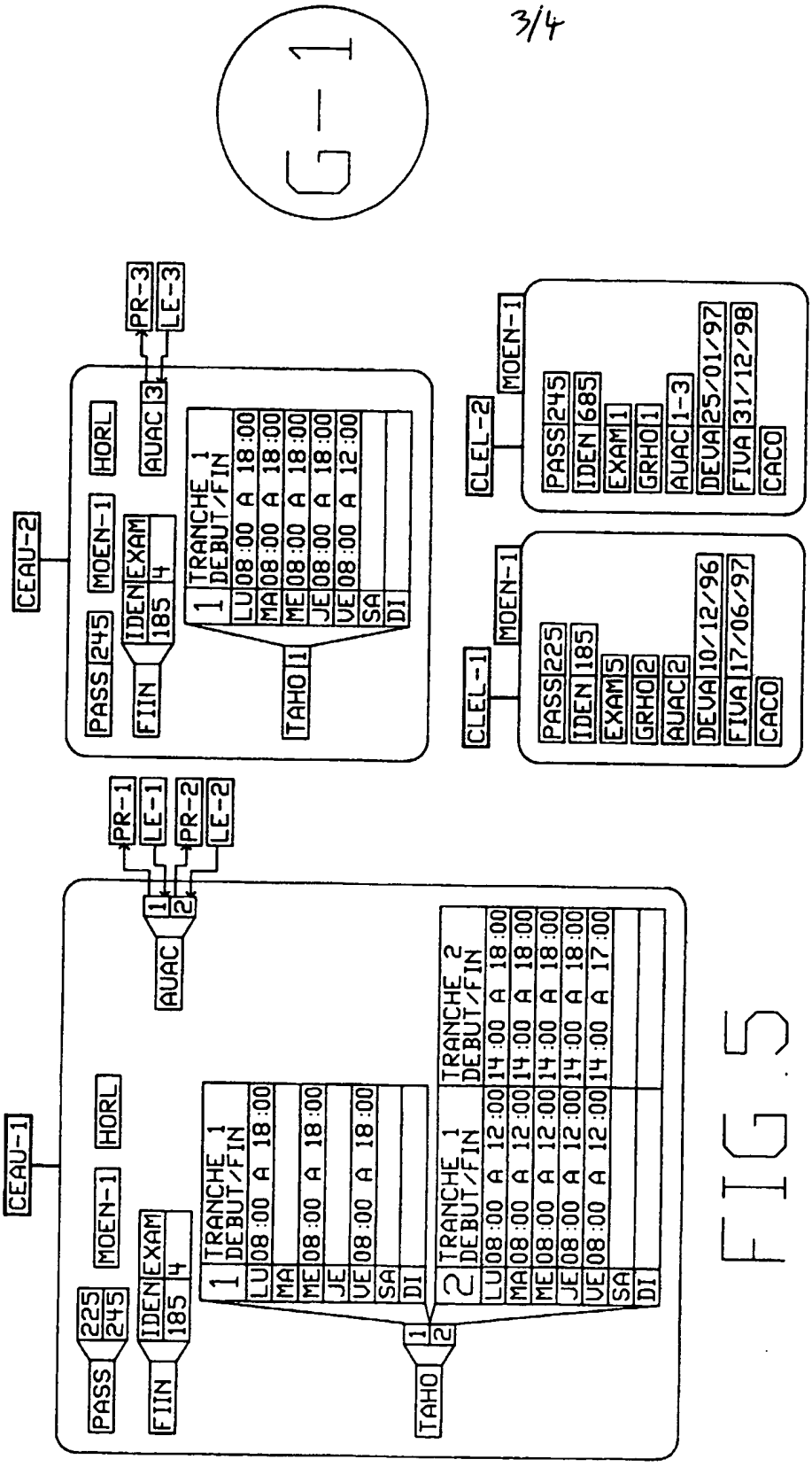
G-1
CEAU-1
HORL
MOEN-1
PASS 225 245
IDEN EXAM 185 4
FIIN
TAHO 1 2
1 TRANCHE 1 DEBUT/FIN
LU 08:00 A 18:00
MA
ME 08:00 A 18:00
JE
VE 08:00 A 18:00
SA
DI
2 TRANCHE 2 DEBUT/FIN
LU 08:00 A 12:00 14:00 A 18:00
MA 08:00 A 12:00 14:00 A 18:00
ME 08:00 A 12:00 14:00 A 18:00
JE 08:00 A 12:00 14:00 A 18:00
VE 08:00 A 12:00 14:00 A 17:00
SA
DI
AUAC 1 2
PR-1
LE-1
PR-2
LE-2
CEAU-2
HORL
MOEN-1
PASS 245
IDEN EXAM 185 4
FIIN
TAHO 1
1 TRANCHE 1 DEBUT/FIN
LU 08:00 A 18:00
MA 08:00 A 18:00
ME 08:00 A 18:00
JE 08:00 A 18:00
VE 08:00 A 12:00
SA
DI
AUAC 3
PR-3
LE-3
CLEL-1
MOEN-1
PASS 225
IDEN 185
EXAM 5
GRHO 2
AUAC 2
DEVA 10/12/96
FIVA 17/06/97
CACO
CLEL-2
MOEN-1
PASS 245
IDEN 685
EXAM 1
GRHO 1
AUAC 1-3
DEVA 25/01/97
FIVA 31/12/98
CACO

FIG 5

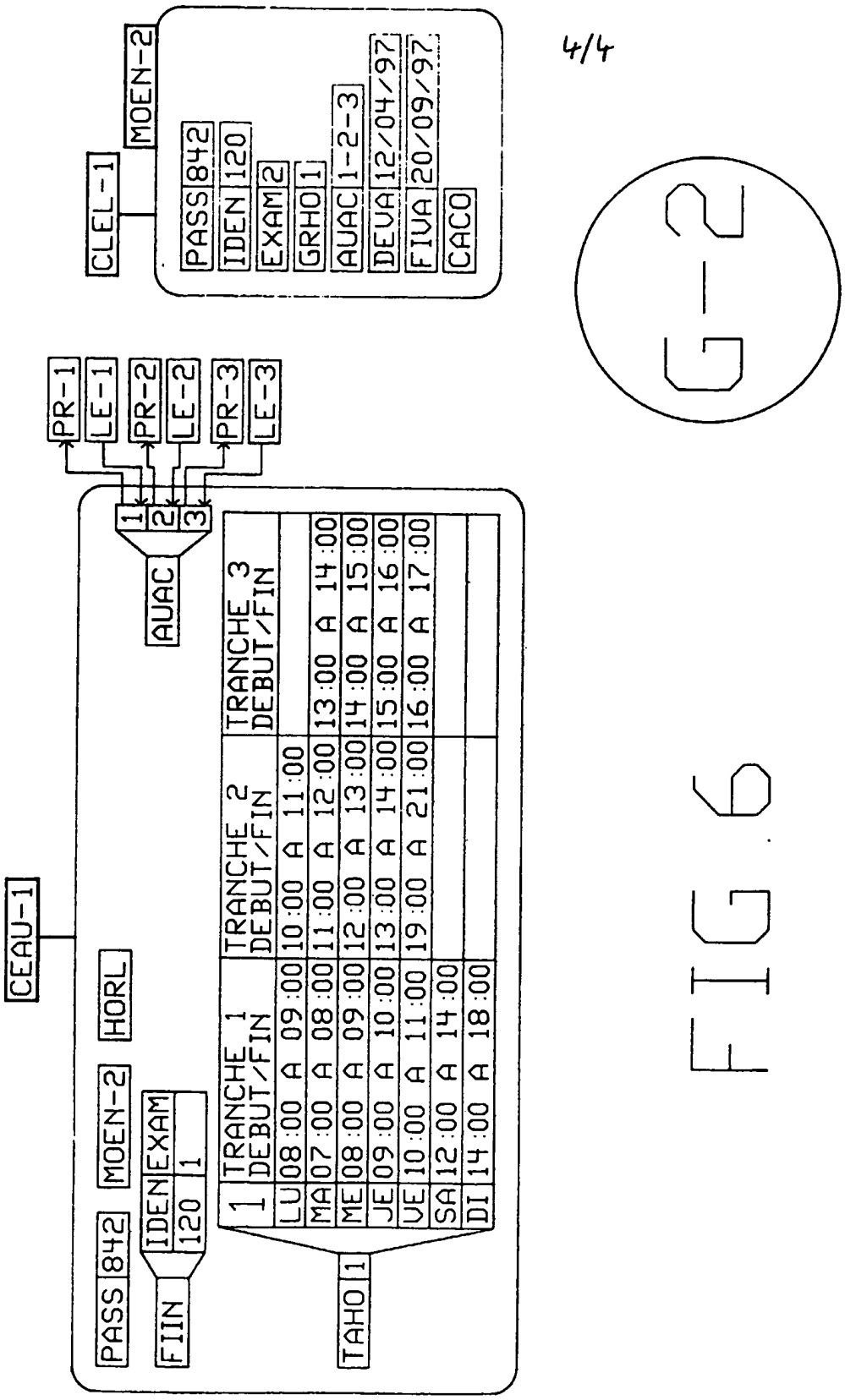
CEAU-1
PASS 842
MOEN-2
HORL
IDEN 120
EXAM 1
FIIN
TAHO 1
1 TRANCHE 1 DEBUT/FIN
LU 08:00 A 09:00
MA 07:00 A 08:00
ME 08:00 A 09:00
JE 09:00 A 10:00
VE 10:00 A 11:00
SA 12:00 A 14:00
DI 14:00 A 18:00
TRANCHE 2 DEBUT/FIN
10:00 A 11:00
11:00 A 12:00
12:00 A 13:00
13:00 A 14:00
14:00 A 15:00
19:00 A 21:00
TRANCHE 3 DEBUT/FIN
13:00 A 14:00
14:00 A 15:00
15:00 A 16:00
16:00 A 17:00
AUAC
1
2
3
PR-1
LE-1
PR-2
LE-2
PR-3
LE-3
CLEL-1
MOEN-2
PASS 842
IDEN 120
EXAM 2
GRHO 1
AUAC 1-2-3
DEVA 12/04/97
FIVA 20/09/97
CACO

FIG 6

G-2